Progress in number theory in the years 1998-2009

Adam Grygiel*

Abstract

We summarize the major results in number theory of the last decade.

1 Introduction

The purpose of the present paper, originally published in Polish (see [19]), is to review briefly nine spectacular achievements belonging to the theory of numbers from the years 1998-2009. We classify these results in the following subjects according to *Mathematical Reviews*:

- Elementary number theory;
- Sequences and sets of integers;
- Diophantine equations;
- Analytic number theory;
- Computational number theory.

I would like to thank the anonymous referee for his remarks improving the paper, and Professors Jerzy Browkin and Andrzej Schinzel for their valuable comments and advice. I am also grateful to Professor Kevin Ford for kindly correcting the statement of his result in the second section, about the Carmichael Conjecture.

2 Elementary number theory

For *Euler's totient function* ϕ the following formula holds

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),$$

in which $p_1, \ldots, p_k$ denote distinct prime factors of n. (Let us remember that by $\phi(a)$ we denote the number of positive integers less than or equal to a that

*The author was partially supported by Dean of the Faculty of Mathematics and Computer Science of the University of Łódź, and the European Social Fund and Budget of State implemented under the Integrated Regional Operational Programme (Project: GRRI-D).

are coprime to a.) In 1922, R.D. Carmichael formulated in [5] an hypothesis, which asserts that there is no integer m such that the equation $\phi(x) = m$ has exactly one solution; this conjecture is still unsubstantiated. Denote by $\mathcal{V}$ the set of values taken by Euler's totient function. In 1998, K. Ford proved in [9] that a prospective counter-example abolishing Carmichael's conjecture satisfies $m > 10^{10^{10}}$, and that if there exists such counter-example, then the set A of these counter-examples has positive relative lower density, that is,

$$\liminf_{N\to\infty} \frac{|A \cap [1, N]|}{|\mathcal{V} \cap [1, N]|} > 0.$$

W. Sierpiński has formulated the following hypothesis (see [34, Ch. VI, 1, p. 252]).

Conjecture 2.1 (Sierpiński 1950) *For any integer $s \geq 2$, there exists such an integer m that the equation $\phi(x) = m$ has exactly s solutions.*

K. Ford and S. Konyagin have proved in [11] the following theorem.

Theorem 2.1 (Ford, Konyagin 1999) *Sierpiński's Conjecture on Euler's totient function holds for even integers.*

Soon after this breakage, K. Ford has proved in [10] Conjecture 2.1. He has used many deep results from sieve theory, e.g. Chen's theorem from [7], which asserts that there exist infinitely many prime numbers p such that $p + 2$ is a product of at least two prime numbers.

3 Sequences and sets of integers

P. Erdős (see [8, p. 11]) has offered \$3000 for a solution of the following still unsolved problem.

Conjecture 3.1 (Erdős 1980) *Any subset A of the positive integers such that $\sum_{n\in A} \frac{1}{n} = \infty$ contains an arithmetic progression of length k, for all k.*

It is known due to Euler that the series of the inverses of all prime numbers divergents. In 1939, J.G. van der Corput proved in [38] that there exist infinitely many arithmetic progressions of prime numbers of length 3. In 1975, E. Szemerédi proved in [35], in a combinatorial way, that any subset of positive integers, with positive upper density, contains arithmetic progression of length k, for all k. Unfortunately, the set $\mathcal{P}$ of all prime numbers has upper density zero. W.T. Gowers has extended Szemerédi's theorem, by using Fourier analysis, to the following result from [16].

Theorem 3.1 (Gowers 2001, Fields Medal 1998) *The maximal length $r_l(n)$ of a progression of integers not exceeding n, containing no arithmetic progression of length l, satisfies*

$$r_l(n) = O\left(\frac{n}{(\ln\ln n)^{c_l}}\right), \quad c_l = 2^{-2^{l+9}}.$$

In 2005, B. Green proved in [17], by the same method, that any set $A \subset \mathcal{P}$ with positive relative upper density, that is, satisfying the condition

$$\limsup_{N\to\infty} \frac{|A \cap [1,N]|}{|\mathcal{P} \cap [1,N]|} > 0,$$

contains infinitely many arithmetic progressions of length 3. By using ergodic methods, jointly with T. Tao he has generalized this fact in [18] to arbitrarily long arithmetic progressions, solving Conjecture 3.1 in the crucial case, when $A = \mathcal{P}$.

Theorem 3.2 (Green, Tao 2008, Fields Medal 2006) *Any set $A \subset \mathcal{P}$ with positive relative upper density contains infinitely many arithmetic progressions of length k, for all k.*

Let $N \in \mathcal{P}$ be a sufficiently large. Let us denote

$$W = \prod_{\substack{p\in\mathcal{P} \\ p\le \ln\ln N}} p.$$

Let us remember that *von Mangoldt's function* Λ is given by

$$\Lambda(n) = \begin{cases} \ln p & \text{if } n = p^l \text{ for some } p \in \mathcal{P} \text{ and positive integer } l, \\ 0 & \text{in the opposite case,} \end{cases}$$

and consider the following modification of this function:

$$\tilde{\Lambda}(n) = \begin{cases} \frac{\phi(W)}{W} \ln(Wn+1) & \text{if } Wn+1 \in \mathcal{P}, \\ 0 & \text{in the opposite case.} \end{cases}$$

A key point in the proof of Theorem 3.2 is a lower evaluation of the expression

$$\frac{1}{N^2} \sum_{n=1}^{N} \sum_{r=1}^{N} \tilde{\Lambda}(n)\tilde{\Lambda}(n+r)\cdots\tilde{\Lambda}(n+(k-1)r).$$

This evaluation implies that there exists in $\mathcal{P}$ an arithmetic progression of the form

$$Wn+1, W(n+r)+1, \ldots, W(n+(k-1)r)+1.$$

The proof of Theorem 3.2 does not follow as to design arithmetic progressions in $\mathcal{P}$ of a given length. In 2008, J. Wróblewski and R. Chermoni found the longest currently known such progression:

$$6171054912832631 + 366384 \times 223092870 \times n, \quad n = 0, \ldots, 24.$$

T. Tao and T. Ziegler have proved in [36], by using ergodic theory, the following generalization of Theorem 3.2.

Theorem 3.3 (Tao, Ziegler 2008) *If $P_1, \ldots, P_k \in \mathbb{Z}[m]$ are integer-valued polynomials such that $P_1(0) = \cdots = P_k(0) = 0$, then any subset of $\mathcal{P}$ with positive relative upper density contains infinitely many sequences of the form $n + P_1(m), \ldots, n + P_k(m)$, with $m > 0$.*

4 Diophantine equations

E. Catalan has formulated in [6] the following hypothesis.

Conjecture 4.1 (Catalan 1844) *Catalan's equation*

$$x^p - y^q = 1,$$

has no solutions in integers $x, y, p, q > 1$ *other than* $3^2 - 2^3 = 1$.

The case of $q = 2$ of Conjecture 4.1 was solved in [26] by V.A. Lebesgue in 1850. In 1964, Chao Ko proved in [25] Conjecture 4.1 for $p = 2$. In 1976, R. Tijdeman proved in [37], by using Baker's method of estimates for linear forms of logarithms, that Catalan's equation has only finitely many solutions. These results were clearly presented in [31] by P. Ribenboim.

In 1990, K. Inkeri (see [23, 24]) proved the following result (the so called *Inkeri's criterion*). Let $p, q \in \mathcal{P}$ be odd integers. If Catalan's equation has a solution in integers $x, y > 1$, then the following alternative holds: $p^{q-1} \equiv 1 \pmod{q^2}$ or q divides the class number of a number field L defined as follows:

$$L = \begin{cases} \mathbb{Q}\left(\sqrt{-p}\right) & \text{if } p \equiv 3 \pmod 4, \\ \mathbb{Q}\left(e^{2i\pi/p}\right) & \text{in the opposite case.} \end{cases}$$

In 2003, P. Mihăilescu proved in [29] that the second term of the alternative in Inkeri's criterion one can drop. More precisely, he has proved the following theorem.

Theorem 4.1 (Mihăilescu 2003) *Let* $p, q \in \mathcal{P}$ *be odd integers. If Catalan's equation has a solution in integers* $x, y > 1$, *then* $p^{q-1} \equiv 1 \pmod{q^2}$ *and* $q^{p-1} \equiv 1 \pmod{p^2}$.

A pair of odd integers $p, q \in \mathcal{P}$, satisfying both congruences in Theorem 4.1, is called a *double Wieferich pair*. There are currently only six such pairs known. In 2004, P. Mihăilescu proved in [30] Conjecture 4.1. A crucial role in his proof is played by the condition $p \not\equiv 1 \pmod q$, which he has proved, by using the double Wieferich pair condition. The original proof was much improved by Y. Bilu (see [3, 4]).

5 Analytic number theory

A. Schinzel has formulated in [33] the following general hypothesis, known as *Schinzel's Hypothesis H*.

Conjecture 5.1 (Schinzel 1958) *Let* $f_1, \ldots, f_k \in \mathbb{Z}[m]$ *be irreducible, integer-valued polynomials, with positive leading coefficients. If for every* $q \in \mathcal{P}$ *we have* $q \nmid f_1(m) \cdots f_k(m)$ *for some* $m \in \mathbb{Z}$, *then* $f_1(n), \ldots, f_k(n) \in \mathcal{P}$ *for infinitely many positive integers* n.

In 1961, A. Schinzel proved in [32] that Conjecture 5.1 implies Conjecture 2.1. Jointly with W. Sierpiński he has also deduced in [33] many other interesting corollaries from Conjecture 5.1, e.g. that there exist arbitrarily long arithmetic progressions of consecutive prime numbers (which is still an open problem). The longest currently known such progression, of length 10, was found by a group associated with M. Toplic in 1998.

Classical Dirichlet's theorem on prime numbers in arithmetic progressions says that, if $f(m) = bm + a$, where $a, b \in \mathbb{Z}$, $a \neq 0$, $b \geq 1$, and $(a, b) = 1$, then $f(n) \in \mathcal{P}$ for infinitely many integers n. In 1978, H. Iwaniec proved in [21] that $n^2 + 1$ is a product of at least two prime numbers for infinitely many integers n. We know currently no polynomial of degree greater than 1, in one variable, which would represent infinitely many prime numbers. Also for $k > 1$ Conjecture 5.1 is completely open problem, even for linear polynomials.

It is known due to Euler (which is the statement of Fermat's theorem on sums of two squares) that a prime number $p > 2$ is a sum of two squares of integers, if and only if $p \equiv 1 \pmod 4$. In particular, $m^2 + n^2 \in \mathcal{P}$ for infinitely many integers m, n. In 1974, H. Iwaniec generalized in [22] the last fact to polynomials of degree 2, in two variables, satisfying some natural assumptions. In 1997, E. Fouvry and H. Iwaniec proved in [12], by using sieve methods, that $m, m^2 + n^2 \in \mathcal{P}$ for infinitely many integers m, n. J. Friedlander and H. Iwaniec have proved in [13], by using Bombieri's asymptotic sieve, that

$$\sum_{m^2+n^4 \leq x} \sum \Lambda(m^2 + n^4) \sim cx^{3/4}, \quad c = \frac{4}{\pi} \int_0^1 (1 - t^4)^{1/2} \mathrm{dt}.$$

This implies the following theorem.

Theorem 5.1 (Friedlander, Iwaniec 1998) *$m^2+n^4 \in \mathcal{P}$ for infinitely many integers m, n.*

D.R. Heath-Brown has proved in [20], by the same method, the following theorem.

Theorem 5.2 (Heath-Brown 2001) *$m^3 + 2n^3 \in \mathcal{P}$ for infinitely many integers m, n.*

Let p_n be the n-th prime number. Let us denote

$$\triangle_1 = \liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\ln p_n}.$$

Until quite lately, the best known evaluation was $\triangle_1 \leq 0.2484$, proven in [28] by H. Maier in 1988. D.A. Goldston, J. Pintz and C.Y. Yıldırım [14] have reached a great breakage in this area. They have proved in [14], by using Selberg's sieve methods, the following theorem.

Theorem 5.3 (Goldston, Pintz, Yıldırım 2009) $\triangle_1 = 0$.

D.A. Goldston, J. Pintz and C.Y. Yıldırım have also proved in [15] the following reinforcement of Theorem 5.3,

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{(\ln p_n)^{1/2}(\ln\ln p_n)^2} < \infty.$$

For fixed $\varepsilon > 0$ let us take sufficiently large integers N, k, and define $h = \varepsilon \ln N$. Let us denote $\mathcal{H}_k = \{h_1, \ldots, h_k\}$, where $h_1, \ldots, h_k$ are integers and $1 \leq h_1 < \ldots < h_k \leq h$, and consider, when a polynomial $P_{\mathcal{H}_k}$ given by $P_{\mathcal{H}_k}(n) = (n+h_1)\cdots(n+h_k)$ has $k+l$ or less distinct prime factors, where $0 \leq l \leq k$. Set

$$\Lambda_R(n;\mathcal{H}_k,l) = \frac{1}{(k+l)!} \sum_{\substack{d \mid P_{\mathcal{H}_k}(n) \\ d \leq R}} \mu(d) \left(\ln\frac{R}{d}\right)^{k+l},$$

where R is a suitable real parameter; let us remember that

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct prime numbers,} \\ 0 & \text{for other } n > 1. \end{cases}$$

Let us consider the following modification of von Mangoldt's function Λ:

$$\hat{\Lambda}(n) = \begin{cases} \ln n & \text{if } n \in \mathcal{P}, \\ 0 & \text{in the opposite case.} \end{cases}$$

A key point in the proof of Theorem 5.3 is a lower evaluation of the expression

$$\sum_{n=N+1}^{2N} \left(\sum_{1\leq h_0 \leq h} \hat{\Lambda}(n+h_0) - \ln(3N) \right) \sum_{1\leq h_1 < \ldots < h_k \leq h} \Lambda_R(n;\mathcal{H}_k,l)^2.$$

This evaluation implies that the interval $(n, n+h)$ contains at least two prime numbers for infinitely many integers n.

6 Computational number theory

In 1983, L.M. Adleman, C. Pomerance and R.S. Rumely published in [1] an algorithm for determining whether a given integer $n > 1$ is a prime. The time complexity of their algorithm equals

$$(\ln n)^{O(\ln\ln\ln n)}.$$

In 2004, M. Agrawal, N. Kayal and N. Saxena published in [2] the first polynomial-time primality test. Their algorithm (the so called *AKS primality test*) executes the following steps.

1. If $n = a^b$ for some integers $a, b > 1$, output „composite".

2. Find the smallest r such that $o_r(n) > (\log_2 n)^2$, where $o_r(n)$ denotes the smallest positive integer k such that $n^k \equiv 1 \pmod{r}$, and $\log_2$ means a logarithm to the base 2.

3. If $1 < (a, n) < n$ for some $a \leq r$, output ,,composite".

4. If $n \leq r$, output ,,primes".

5. For $1 \leq a \leq \lfloor \sqrt{\phi(r)} \log_2 n \rfloor$ do: if $(X+a)^n \neq X^n + a$ in $(\mathbb{Z}/n\mathbb{Z})[X]/(X^r - 1)$, output ,,composite".

6. Output ,,primes".

Theorem 6.1 (Agrawal, Kayal, Saxena 2004) *The AKS primality test returns ,,primes" if and only if $n \in \mathcal{P}$. The time complexity of this algorithm equals $O\left((\ln n)^{\frac{21}{2}+\varepsilon}\right)$, for any $\varepsilon > 0$.*

The main difficulty in the proof of correctness of the AKS primality test lies in the implication that, if the above algorithm returns ,,primes", then $n \in \mathcal{P}$. It was shown elementarily (see [2, Lemma 4.3]) that there exists $r \leq \max\{3, \lceil (\log_2 n)^5 \rceil\}$ such that $o_r(n) > (\log_2 n)^2$. Since $o_r(n) > 1$, there exists such prime factor p of n that $o_r(p) > 1$. A further part of the proof is based on the equality

$$x^r - 1 = \prod_{d|r} \Phi_d(x),$$

in which $\Phi_d \in (\mathbb{Z}/p\mathbb{Z})[x]$ denotes the d-th cyclotomic polynomial. Let $h \in (\mathbb{Z}/p\mathbb{Z})[x]$ be an irreducible factor of Φ_r. Then, the ring $\mathbb{F} := (\mathbb{Z}/p\mathbb{Z})[x]/(h(x))$ is a finite field of order p^d, where d is the degree of h. A key point in the proof of Theorem 6.1 is a lower and upper evaluation of the order of the cyclic subgroup $\mathbb{F}$ generated multiplicatively by the elements

$$x, x+1, x+2, \ldots, x + \lfloor \sqrt{\phi(r)} \log_2 n \rfloor,$$

under the assumption that n is not a power of p. It follows from these evaluations that $n = p$.

H.W. Lenstra, Jr. and C. Pomerance have modificated in [27] the AKS primality test for obtaining a deterministic primality test with the time complexity $O\left((\ln n)^{6+\varepsilon}\right)$, for any $\varepsilon > 0$.

References

[1] L.M. Adleman, C. Pomerance, R.S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. **117** (1983), no. 1, 173–206.

[2] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Ann. of Math. **160** (2004), no. 2, 781–793.

[3] Y.F. Bilu, *Catalan's conjecture (after Mihăilescu)*, Astérisque **294** (2004), vii, 1–26.

[4] Y.F. Bilu, *Catalan without logarithmic forms (after Bugeaud, Hanrot and Mihăilescu)*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 69–85.

[5] R.D. Carmichael, *Note on Euler's ϕ-function*, Bull. Amer. Math. Soc. **28** (1922), no. 3, 109–110.

[6] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. Reine Angew. Math. **27** (1844), 192.

[7] J.R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.

[8] P. Erdős, R.L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], vol. 28, Université de Genéve L'Enseignement Mathématique, Geneva, 1980.

[9] K. Ford, *The distribution of totients*, The Ramanujan J. **2** (1998), no. 1-2, 67–151.

[10] K. Ford, *The number of solutions of $\phi(x) = m$*, Ann. of Math. **150** (1999), no. 1, 283–312.

[11] K. Ford, S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 795–803.

[12] E. Fouvry, H. Iwaniec, *Gaussian primes*, Acta Arith. **79** (1997), no. 3, 249–287.

[13] J. Friedlander, H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. of Math. **148** (1998), no. 3, 945–1040.

[14] D.A. Goldston, J. Pintz, C.Y. Yıldırım, *Primes in Tuples I*, Ann. of Math. **170** (2009), no. 2, 819–862.

[15] D.A. Goldston, J. Pintz, C.Y. Yıldırım, *Primes in Tuples II*, preprint.

[16] W.T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588.

[17] B. Green, *Roth's theorem in the primes*, Ann. of Math. **161** (2005), no. 3, 1609–1636.

[18] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. **167** (2008), no. 2, 481–547.

[19] A. Grygiel, *Progress in number theory in the years 1998-2009*. (Polish), Wiad. Mat. **46** (2010), no. 1, 17–26.

[20] D.R. Heath-Brown, *Primes represented by* x^3+2y^3, Acta Math. **186** (2001), no. 1, 1–84.

[21] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171–188.

[22] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta Arith. **24** (1973/74), 435–459.

[23] K. Inkeri, *On Catalan's problem*, Acta Arith. **9** (1964), 285–290.

[24] K. Inkeri, *On Catalan's conjecture*, J. Number Theory **34** (1990), no. 2, 142–152.

[25] Ch. Ko, *On the Diophantine equation* $x^2 = y^n + 1$*;* $xy \neq 0$, Sci. Sinica **14** (1964), 457–460.

[26] V.A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. **9** (1850), 178–181.

[27] H.W. Lenstra, Jr., C. Pomerance, *Primality testing with Gaussian periods*, preprint.

[28] H. Maier, *Small differences between prime numbers*, Michigan Math. J. **35** (1988), no. 3, 323–344.

[29] P. Mihăilescu, *A class number free criterion for Catalan's conjecture*, J. Number Theory **99** (2003), no. 2, 225–231.

[30] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[31] P. Ribenboim, *Catalan's conjecture*, Academic Press, Inc., Boston, MA, 1994.

[32] A. Schinzel, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961/1962), 1–8.

[33] A. Schinzel, W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum **5** (1958), 259.

[34] W. Sierpiński, *Elementary Theory of Numbers*, PWN, Warszawa; North Holland, Amsterdam, 1987.

[35] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

[36] T. Tao, T. Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008), no. 2, 213–305.

[37] R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), no. 2, 197–209.

[38] J.G. van der Corput, *Über Summen von Primzahlen und Primzahlquadraten*, Math. Ann. **116** (1939), 1–50.

Faculty of Mathematics and Computer Science, University of Łódź, Banacha 22, 90-238 Łódź, Poland
A.Grygiel@math.uni.lodz.pl